# IBM Watson Health Core

Termenii de Utilizare ("TdU") sunt alcătuiţi din aceşti Termeni de Utilizare IBM – Termeni Specifici Ofertei SaaS ("Termenii Specifici Ofertei SaaS") şi un document intitulat Termenii de Utilizare IBM – Termeni Generali ("Termenii Generali"), disponibil la următorul URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

În eventualitatea unui conflict, Termenii Specifici Ofertei SaaS vor prevala faţă de Termenii Generali. Prin comandarea, accesarea sau utilizarea IBM SaaS, Clientul este de acord cu Termenii de Utilizare.

Termenii de Utilizare sunt guvernaţi de IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement sau IBM International Agreement for Selected IBM SaaS Offerings, după caz ("Contractul"), care împreună cu Termenii de Utilizare reprezintă acordul complet.

## 1. IBM SaaS

Aceşti Termeni Specifici Ofertei SaaS acoperă următoarele oferte IBM SaaS:

- IBM Watson Health Core
- IBM Watson Health Core Access
- IBM Watson Health Core Terminology Service

## 2. Indicii de Măsurare pentru Tarifare

IBM SaaS este vândut în baza unuia dintre următorii indici de măsurare pentru tarifare, după cum este specificat în Documentul Tranzacţional:

a. **Acces** – este o unitate de măsură pentru obţinerea IBM SaaS. Un Acces înseamnă dreptul de a utiliza IBM SaaS. Clientul trebuie să obţină un singur drept Acces în vederea utilizării IBM SaaS pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (PoE) sau Documentul Tranzacţional al Clientului.

b. **Individ** – este o unitate de măsură pentru obţinerea IBM SaaS. Un Individ este un singur lucru sau o singură persoană. Trebuie obţinute drepturi suficiente pentru a acoperi fiecare Individ accesat sau gestionat de IBM SaaS pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (Proof of Entitlement - PoE) sau Documentul Tranzacţional al Clientului.

   Pentru scopurile acestui IBM SaaS, un Individ poate fi o persoană, un dispozitiv sau o aplicaţie mobilă ale cărei date sunt gestionate de IBM SaaS.

c. **Instanţă** – este o unitate de măsură pentru obţinerea IBM SaaS. O Instanţă este accesul la o configuraţie IBM SaaS specifică. Trebuie obţinute drepturi suficiente pentru fiecare Instanţă IBM SaaS făcută disponibilă pentru acces şi utilizare pe durata perioadei de măsurare specificate în Documentul Tranzacţional al Clientului.

## 3. Tarife şi Facturare

Suma de plată pentru IBM SaaS este specificată într-un Document Tranzacţional.

### 3.1 Tarife Lunare Parţiale

Un tarif lunar parţial, după cum este specificat în Documentul Tranzacţional, poate fi evaluat prin proratare.

### 3.2 Tarife pentru Excedent

Dacă utilizarea reală de către Client a IBM SaaS pe durata perioadei de măsurare depăşeşte dreptul de utilizare specificat în PoE, Clientul va fi facturat pentru excedent după cum este specificat în Documentul Tranzacţional.

## 4. Opţiunile pentru Termen şi Reînnoire

Termenul IBM SaaS începe la data la care IBM anunţă Clientul că acesta are acces la mediul de operare Pilot al IBM SaaS, după cum este specificat în Documentul de Comandă. Perioada de abonare pentru drepturile Individ începe atunci când IBM anunţă Clientul că acesta are acces la mediul de operare Producţie. Documentul de Comandă va specifica dacă oferta IBM SaaS este reînnoită automat, va fi furnizată mai departe pe bază de utilizare continuă sau se va termina la sfârşitul termenului.

În cazul reînnoirii automate, cu excepţia situaţiei în care Clientul, cu cel puţin 90 de zile înainte de expirarea termenului, trimite o notificare scrisă prin care anunţă că nu doreşte reînnoirea, oferta IBM SaaS va fi reînnoită automat pentru termenul specificat în PoE.

În cazul utilizării continue, oferta IBM SaaS va continua să fie disponibilă, de la lună la lună, până când Clientul trimite, cu 90 de zile înainte, o notificare scrisă privind terminarea. După această perioadă de 90 de zile, oferta IBM SaaS va rămâne disponibilă până la sfârşitul lunii calendaristice.

## 5. Suport Tehnic

IBM va face disponibilă publicaţia IBM Software as a Service Support Handbook, care conţine informaţii de contact pentru suport tehnic şi alte informaţii şi procese. Informaţiile de contact pentru suport tehnic şi alte detalii privind operaţiunile de suport pot fi găsite în IBM SaaS Support Handbook, la: https://support.ibmcloud.com.

Cererile de suport tehnic şi configurare simplă pentru IBM SaaS sunt furnizate prin expediere electronică. Suportul Tehnic este furnizat cu IBM SaaS şi nu este disponibil ca ofertă separată.

**Când este raportată o problemă, documentaţia sau informaţiile trimise nu pot conţine Informaţii Personale, cum ar fi Informaţiile Protejate privind Sănătatea şi Informaţiile Personale Sensibile.**

## 6. Definiţii

**Legi Aplicabile** – înseamnă orice legi, statute sau dispoziţii legislative, reguli, reglementări, directive, mandate, decrete sau alte cerinţe ale unei autorităţi guvernamentale sau ale oricăror standarde general acceptate în industrie care au legătură cu aplicarea acestor Termeni de Utilizare

**API** – înseamnă interfaţă de programare a aplicaţiilor, care este un set de rutine, protocoale şi instrumente pentru construirea aplicaţiilor software. Un API specifică modul în care trebuie să interacţioneze componentele software. API-urile sunt utilizate atunci când sunt programate componentele interfeţei grafice de utilizator.

**Administrator Autorizat** – este orice angajat al Clientului, contractor aprobat al Clientului, persoană sau grup responsabil pentru gestionarea întreţinerii şi asigurarea operării fiabile a platformei. Responsabilităţile pot include configurarea, suportul şi gestionarea utilizatorilor şi conturilor. Administratorul poate fi şi un investigator clinic, responsabil pentru setarea unui studiu în sistemul Watson Health.

**Individ Autorizat** – este orice persoană, aplicaţie mobilă sau dispozitiv autentificat care a primit drept de acces pentru trimiterea datelor către Watson Health Core. Un Individ Autorizat poate fi Clientul sau participanţi la studiu, clienţi sau pacienţi ai Clientului.

**Legi Aplicabile pentru Client privind Datele** – înseamnă Legile privind Datele care sunt aplicabile pentru îndeplinirea de către Client a obligaţiilor care îi revin în baza Contractului, Documentelor Asociate şi a Descrierilor de Serviciu, Documentelor de Comandă şi Ordinelor de Lucru aplicabile între Părţi.

**Datele Clientului** – înseamnă orice intrări de date în IBM SaaS, realizate de către Client sau pentru el, indiferent dacă sunt date deţinute de Client sau date introduse de sau în numele unui client al Clientului sau oricărei terţe părţi, şi care includ orice date de la un dispozitiv de sănătate terţă parte.

**Legi privind Datele** – înseamnă orice Legi Aplicabile care se referă la protecţia, confidenţialitatea sau securitatea datelor.

**Subiectul Datelor** – înseamnă o persoană identificată sau identificabilă, la care se referă Datele Personale.

**Centru de Date Desemnat** – înseamnă centrul (centrele) de date specificat în Documentul Tranzacţional pentru centrele de date primare şi de recuperare după dezastru, care rulează instanţa IBM SaaS a Clientului, dacă este aplicabil.

**Date de Sănătate** – înseamnă orice date sau informaţii, inclusiv imagini, care reprezintă Informaţii Personale privind sănătatea.

**Activat pentru Date de Sănătate** – înseamnă, referitor la IBM SaaS, abilitatea IBM SaaS de a respecta standardele aplicabile privind securitatea şi confidenţialitatea, legile şi reglementările din Jurisdicţiile Incluse în Scop pentru Datele de Sănătate, inclusiv specificaţiile pentru implementare prevăzute în Partea 164, Sub-părţile A şi C, ale normelor pentru aplicarea HIPAA (conform modificărilor din Legea HITECH) şi alte Legi Aplicabile privind Datele de Sănătate, dar nu înseamnă că IBM acţionează în calitate de Asociat de Afaceri sau Controlor de Date.

**HIPAA** – înseamnă legea Health Insurance Portability and Accountability Act din 1996, cu amendamente, inclusiv legea Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act din 2009 ("Legea HITECH"), anumite reglementări promulgate în baza HIPAA de către United States Department of Health and Human Services, în 45 C.F.R. Părţile 160 şi 164, şi anumite reglementări promulgate în temeiul Legii HITECH Act.

**Legi Aplicabile pentru IBM privind Datele** – înseamnă Legile privind Datele care sunt aplicabile pentru îndeplinirea de către IBM a obligaţiilor care îi revin în baza Contractului, Documentelor Asociate şi a Descrierilor de Serviciu, Documentelor de Comandă şi Ordinelor de Lucru aplicabile între Părţi.

**Personal IBM** – înseamnă (a) IBM, Afiliatele sale şi subcontractorii săi, precum şi angajaţii acestora; şi (b) orice furnizor terţă parte, în fiecare caz în care acesta furnizează servicii în numele IBM în baza Contractului şi a Documentelor Asociate aplicabile sau căruia IBM i-a autorizat în alt fel accesul la Datele Personale ale Clientului.

**Ţări Incluse în Scop** – înseamnă cele 28 de state membre ale Uniunii Europene şi Elveţia, precum şi ţările pe care IBM le poate adăuga în această listă, periodic.

**Date Personale** sau **Informaţii Personale** – înseamnă informaţiile, pe orice mediu şi în orice format, inclusiv înregistrările electronice şi pe hârtie, care au legătură cu o persoană identificată sau identificabilă, o "persoană identificabilă" fiind cineva care poate fi identificat, direct sau indirect, în particular, prin asocierea cu un număr de identificare sau unul sau mai mulţi factori specifici identităţii sale fizice, fiziologice, mentale, economice, culturale sau sociale.

**Proces** şi variantele sale, cum ar fi **procesare** (indiferent că sunt scrise cu majusculă sau fără) – înseamnă orice operaţiune sau set de operaţiuni realizat asupra datelor, indiferent că mijloacele sunt automate sau nu, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, distribuire sau alt mijloc de a le face disponibile, alinierea sau combinarea, blocarea, ştergerea sau distrugerea.

**Date Procesate** – înseamnă orice date, confidenţiale sau informaţii sau materiale proprietate, inclusiv Datele de Sănătate şi Datele Personale, care sunt procesate de IBM în baza Contractului, a unui Document Asociat şi/sau a unei Descrieri de Serviciu, a unui Document de Comandă şi/sau Ordin de Lucru.

**Incident de Securitate** – are semnificaţia stabilită în Anexa pentru Securitate şi Continuitatea Activităţii.

## 7. Gestionarea Conturilor

IBM SaaS este accesibil numai pentru utilizatorii autorizaţi ai Clientului ("**Administratori Autorizaţi**" sau "**Indivizi Autorizaţi**"). Clientul va controla conturile autorizate să acceseze IBM SaaS, care pot include aplicaţii autorizate, personalul Clientului, furnizori de servicii terţă parte sau contractori ai Clientului, şi este responsabil în mod exclusiv pentru (i) controlul tuturor utilizatorilor autorizaţi, incluzând, dar fără limitare, verificarea identităţii utilizatorului autorizat; şi (ii) asigurarea că numai utilizatorii autorizaţi accesează IBM SaaS.

Indivizii Autorizaţi care sunt clienţi, pacienţi sau participanţi la studiu ai Clientului pot primi acces numai în scopul încărcării datelor în IBM SaaS, caz în care astfel de Indivizi Autorizaţi nu vor avea acces la IBM SaaS.

## 8. Confidenţialitatea

### 8.1 Cerinţe Generale

În relaţia dintre Părţi, Clientul este controlorul unic al Datelor Personale ale Clientului şi Clientul desemnează IBM ca un procesor de date. În conformitate cu Legile Aplicabile privind Datele, Clientul are dreptul de a furniza către IBM instrucţiuni privind procesarea de către IBM a Datelor Personale ale Clientului.

În cursul procesării de către IBM a Datelor Personale ale Clientului, IBM:

a. va respecta toate Legile Aplicabile pentru IBM privind Datele; şi

b. nu va combina Datele Personale ale Clientului cu datele din alte surse, exceptând:

- cazul în care este necesar pentru a furniza IBM SaaS şi nu pentru alte scopuri, decât la solicitarea expresă a Clientului de a face aceasta; sau
- situaţiile conforme termenilor din aceşti Termeni de Utilizare şi din Anexa pentru Securitate şi Continuitatea Activităţii.

În cursul procesării de către IBM a Datelor Personale ale Clientului, Clientul:

a. va respecta toate Legile Aplicabile pentru Client privind Datele;

b. va fi responsabil pentru toate comunicările Clientului cu Afiliatele Clientului, pacienţii, utilizatorii finali, Subiecţii Datelor şi/sau alte terţe părţi ale Clientului;

c. va încheia acorduri de procesare a datelor cu controlorii săi care trebuie să permită ca IBM, ca procesor de date, şi subprocesorii săi să proceseze orice Date Personale ale Clientului; şi

d. va servi ca punct unic de contact pentru IBM şi va fi responsabil în mod exclusiv pentru coordonarea internă, examinarea şi trimiterea către IBM a instrucţiunilor sau cererilor Afiliatelor Clientului care sunt controlori. IBM nu va avea obligaţia de a informa sau notifica nicio Afiliată a Clientului că este un controlor, atunci când a furnizat Clientului această informaţie sau notificare. IBM are dreptul de a refuza orice instrucţiuni furnizate direct de orice Afiliată a Clientului care este un controler ce nu este Client.

Nicio parte nu va fi obligată să acţioneze prin încălcarea Legilor sale Aplicabile privind Datele.

## 8.2 Drepturile privind Datele Clientului

Clientul declară şi garantează că (a) deţine datele care vor fi introduse în IBM SaaS sau (b) a obţinut şi este responsabil pentru a menţine, toate drepturile, permisiunile, consimţămintele şi autorizările necesare pentru ca IBM să aibă dreptul de a accesa, utiliza şi dezvălui Datele Clientului în conformitate cu termenii stabiliţi în aceşti Termeni de Utilizare sau Contract, sau după cum este altfel necesar pentru ca IBM să furnizeze IBM SaaS. De asemenea, Clientul declară şi garantează că Datele Clientului vor fi referitoare numai la (a) persoane cu reşedinţa în Statele Unite şi aceste date vor fi introduse apoi în IBM SaaS într-un centru de date din Statele Unite sau (b) persoane cu reşedinţa în una sau mai multe ţări Incluse în Scop şi aceste date vor fi introduse apoi în IBM SaaS în Centrele de Date Desemnate.

## 8.3 Serviciile şi Responsabilităţile privind Datele

a. Clientul este de acord să realizeze analize, sau să solicite ca IBM să realizeze analize, asupra Datelor Clientului în legătură cu activităţile care sunt "operaţiuni de asigurare a sănătăţii" sau "cercetări" ale Clientului, după cum sunt definite acestea în baza HIPAA şi/sau a altor termeni similari din alte Legi Aplicabile privind Datele, şi să utilizeze Datele Clientului, sau să solicite ca IBM să utilizeze Datele Clientului, numai în conformitate cu toate cerinţele relevante (de exemplu, în cazurile în care este necesară o determinare sau renunţare Institutional Review Board), în baza acestora şi a altor Legi Aplicabile pentru Client privind Datele.

b. Client este singurul responsabil pentru obţinerea oricăror şi tuturor înregistrărilor, consimţămintelor, autorizărilor şi permisiunilor cerute de Legile Aplicabile pentru Client, în fiecare Ţară Inclusă în Scop aplicabilă, incluzând, fără limitare, HIPAA şi orice alte legi, reguli şi reglementări aplicabile privind confidenţialitatea şi securitatea datelor, pentru introducerea Datelor Clientului în IBM SaaS şi utilizarea şi dezvăluirea în baza acestor Termeni de Utilizare şi a Contractului, de către Client şi de către IBM şi subcontractorii acceptaţi de IBM. IBM nu va avea nicio responsabilitate privind monitorizarea momentelor în care astfel de înregistrări, consimţăminte, autorizări şi permisiuni sunt primite sau solicitate.

c. Clientul este responsabil în mod exclusiv pentru asigurarea că introducerea Datelor Clientului în IBM SaaS este limitată la datele privind persoanele cu reşedinţa în Statele Unite sau într-o ţară Inclusă în Scop aplicabilă.

d. IBM va avea centre de suport, cu personal instruit cu privire la HIPAA şi alte Legi Aplicabile pentru IBM privind Datele, pentru datele din ţările Incluse în Scop.

## 8.4 Măsurile de Securitate şi Incidentele de Securitate

a. IBM va implementa, va menţine şi va respecta măsurile cu caracter tehnic şi organizaţional, inclusiv procesele şi procedurile organizaţionale şi orice obligaţii specifice privind securitatea, prevăzute sau referite în aceşti Termeni de Utilizare şi Anexa pentru Securitate şi Continuitatea Activităţii, pentru a proteja Datele Personale ale Clientului faţă de utilizarea sau accesul neautorizat, pierderea accidentală, daune, modificarea, distrugerea, furtul sau dezvăluirea neautorizată.

b. Dacă IBM detectează un Incident de Securitate (după cum este definit de Anexa pentru Securitate şi Continuitatea Activităţii) ce implică Date Procesate ale Clientului, IBM va informa Clientul în conformitate cu termenii din Anexa pentru Securitate şi Continuitatea Activităţii şi Legile Aplicabile pentru IBM privind Datele, iar această notificare va include informaţii privind impactul cunoscut asupra Clientului sau oricăror Subiecţi ai Datelor (dacă există) care au fost afectaţi de respectivul Incident de Securitate şi acţiunea de corecţie efectuată sau propusă pentru a fi efectuată de IBM.

## 8.5 Primirea Întrebărilor şi Reclamaţiilor

IBM va trimite Clientului o notificare scrisă şi, în măsura în care este permis de Legile Aplicabile pentru IBM privind Datele, nu mai târziu de cinci (5) zile lucrătoare după ce IBM Watson Health Data Privacy Officer a primit orice întrebare, comunicare sau reclamaţie trimisă către IBM, în legătură cu Datele Personale ale Clientului, de la:

a. orice Subiect al Datelor, cu privire la Datele Personale despre respectivul Subiect al Datelor, procesate de IBM. Clientul va răspunde oricăror cereri de la Subiecţii Datelor, iar IBM va respecta orice instrucţiuni rezonabile ale Clientului privind asistenţa acordată Clientului pentru a răspunde acestor cereri. Dacă Legile Aplicabile pentru IBM impun aceasta, IBM poate răspunde direct unor astfel de cereri, cu condiţia ca IBM să notifice Clientul în prealabil despre orice astfel de răspuns şi să se coordoneze în mod rezonabil cu Clientul cu privire la forma şi conţinutul răspunsului, când este permis de Legile Aplicabile pentru IBM sau este posibil în alt fel;

b. orice autoritate legală sau de reglementare, cu privire la Procesarea de către IBM a oricăror Date Personale ale Clientului, cu condiţia ca IBM să poată răspunde unor astfel de cereri, primite de la o agenţie guvernamentală cu o citaţie sau alt document legal similar, ce solicită dezvăluirea de către IBM sau conformarea cu altă cerinţă a Legii Aplicabile privind Datele, cu condiţia ca IBM să notifice Clientul în prealabil despre orice astfel de dezvăluire şi să se coordoneze în mod rezonabil cu Clientul cu privire la forma şi conţinutul răspunsului, dacă este permis de lege sau este posibil în alt fel.

## 8.6 Procesarea Datelor Personale ale Clientului

IBM va restricţiona dezvăluirea Datelor Personale ale Clientului, către Personalul IBM care poate fi necesar pentru asistenţă la furnizarea Serviciilor.

IBM va respecta orice cerere rezonabilă din partea Clientului, prin care se solicită ca IBM să amendeze, să corecteze, să şteargă sau să blocheze Datele Personale ale Clientului în conformitate cu Legea Aplicabilă.

La cererea oricărei Părţi, IBM, Clientul sau Afiliatele lor vor încheia contracte standard, cerute de lege, privind protecţia Datelor Personale ale Client. Părţile sunt de acord (şi se vor asigura că respectivele lor Afiliate sunt de acord) că astfel de contracte vor respecta limitarea şi excluderile privind răspunderea din acest Contract, în cea ce priveşte reclamaţiile între Părţi. Părţile vor coopera pentru a încheia (şi se vor asigura că Afiliatele Părţilor vor încheia) contracte şi vor respecta termenii conveniţi, după cum cer Legile Aplicabile pentru Date.

## 8.7 Returnarea Datelor Personale ale Clientului

La expirarea sau terminarea Contractului, IBM va înceta, şi va determina Personalul IBM să înceteze, utilizarea sau procesarea oricăror Informaţii Proprietate ale Clientului şi a oricăror Date Personale ale Clientului şi, la alegerea sau cererea Clientului:

a. va returna cu promptitudine, în formatul şi pe mediul de stocare solicitate, în mod rezonabil, de Client, toate Informaţiile Proprietate ale Clientului şi Datele Personale ale Clientului pe care IBM le stochează în mod electronic şi, la confirmarea primirii lor de către Client, va şterge sau va distruge Informaţiile Proprietate ale Clientului şi Datele Personale ale Clientului, inclusiv copiile sau backup-urile, sau se va asigura în alt mod că acestea nu mai pot fi niciodată citite sau descifrate. IBM poate aplica tarife pentru mediile de stocare şi anumite activităţi realizate la cererea Clientului (cum ar fi furnizarea Informaţiilor Proprietate ale Clientului şi a Datelor Personale ale Clientului într-un format specific sau distrugerea Informaţiilor Proprietate ale Clientului şi a Datelor Personale ale Clientului într-o anumită manieră); şi

b. va şterge sau va distruge în mod direct Informaţiile Proprietate ale Clientului şi Datele Personale ale Clientului, inclusiv copiile sau backup-urile, sau se va asigura în alt mod că acestea nu mai pot fi niciodată citite sau descifrate.

### 8.8 Contractul cu Asociatul de Afaceri

În măsura în care este permis sau cerut de HIPAA, IBM şi Clientul vor încheia Contractul cu Asociatul de Afaceri ("CAA"), care va guverna obligaţiile IBM, ca Asociat de Afaceri al Clientului, privind furnizarea IBM SaaS. Fără a limita obligaţiile exprese ale IBM în baza Contractului, şi a CAA, dacă este aplicabil, Clientul ia la cunoştinţă şi este de acord că este responsabil pentru determinarea aplicabilităţii şi conformităţii cu toate Legile Aplicabile şi cerinţele de licenţiere privind utilizarea de către Client sau alte activităţi ale sale legate de IBM SaaS (inclusiv utilizarea Utilizatorilor Autorizaţi sau alte activităţi ale acestora).

### 8.9 Addendum pentru Procesarea Datelor în Uniunea Europeană

În cazul în care Clientul solicită ca IBM să proceseze Date Personale în Uniunea Europeană, IBM şi Clientul vor încheia un Addendum pentru Procesarea Datelor, ce va include, după cum este cazul, Clauze pentru Modelul UE, cu clauzele opţionale înlăturate.

## 9. Termeni Suplimentari pentru Oferta IBM SaaS

### 9.1 Securitatea

Acest IBM SaaS respectă principiile IBM privind securitatea şi confidenţialitatea datelor pentru IBM SaaS, care sunt disponibile la http://www.ibm.com/cloud/data-security, şi termenii suplimentari specificaţi mai jos şi în Anexa pentru Securitate şi Continuitatea Activităţii a acestor Termeni de Utilizare. Nicio modificare a principiilor IBM privind securitatea şi confidenţialitatea datelor nu va afecta securitatea IBM SaaS.

IBM Watson Health Core implementează politici, standarde şi procese de securitate bazate pe cadrul de lucru ISO 27001, după cum se descrie în continuare, în Descrierea Securităţii. Printre capabilităţile sale de securitate, soluţia implementează următoarele:

a. Zone de Operare Securizate

   IBM Watson Health Core implementează strategie amplă de apărare, utilizând mai multe zone de securitate, pentru gestionarea punctelor de integrare cloud, cum ar fi adoptarea şi dezvoltarea aplicaţiilor personalizate.

b. Criptarea

   Toate Datele Clientului sunt criptate static şi dinamic. Toate datele în tranziţie către şi dinspre IBM Watson Health Core sunt criptate. Un serviciu partajat asigură gestionarea cheilor de criptare. Clientul este responsabil pentru întreaga conectivitate şi calitatea reţelei între IBM Watson Health Service serverul proxy al Clientului.

c. Monitorizarea Evenimentelor de Securitate

   IBM utilizează platforma sa de inteligenţă a securităţii pentru gestionarea informaţiilor şi evenimentelor de securitate, gestionarea istoricelor, analiza criminalistică a incidentelor, detectarea ameninţărilor şi gestionarea vulnerabilităţilor.

d. Gestionarea Identităţilor

   - Watson Health Core acceptă furnizori de identităţi bazaţi pe standarde deschise, pentru populaţii mari de pacienţi şi utilizatori, folosind OpenID Connect.
   - În cazul populaţiilor de utilizatori pentru care IBM este furnizorul de identităţi, Watson Health Core utilizează servicii de director corespunzătoare şi capabilităţi de gestionare a identităţilor pentru realizarea autentificării.

e. Autentificare Puternică şi Acces Bazat pe Roluri

   - Watson Health Core permite autentificarea prin SAML, ca mecanism utilizat de Clienţi pentru a-şi integra serviciile SSO (Single Sign On) sau de director.
   - Watson Health Core utilizează o soluţie de gestionare a accesului şi componente conexe pentru a gestiona politicile de securitate, când este necesar.
   - Watson Health Core are inclus suport pentru autentificarea cu doi factori bazată pe software.
   - Watson Health Core asigură un control de bază al accesului, bazat pe roluri, după cum este necesar; Watson Health Core are inclus suport pentru configurarea studiului, profilurilor de utilizator, rolurilor şi grupurilor de utilizatori, prin interfeţe de programare a aplicaţiilor ("API" sau "API-uri") care permit accesul bazat pe roluri.

## 9.2 Cookie-uri

Clientul este conştient şi acceptă că IBM poate, ca parte a operării normale şi asigurării suportului pentru IBM SaaS, să colecteze informaţii personale de la Client (angajaţii şi contractorii dumneavoastră) privind utilizarea IBM SaaS, prin urmărire şi alte tehnologii. IBM face aceasta pentru a colecta statistici privind utilizarea şi informaţii despre eficienţa IBM SaaS, în vederea îmbunătăţirii experienţei de utilizator şi/sau pentru ajustarea interacţiunilor cu Clientul. Clientul confirmă că va obţine sau va avea consimţământul pentru a permite ca IBM să proceseze informaţiile personale colectate pentru scopul menţionat mai sus, în cadrul IBM, în alte companii IBM şi în cele ale subcontractorilor săi, în care noi sau subcontractorii noştri ne desfăşurăm activitatea, în conformitate cu legile aplicabile. IBM se va conforma solicitărilor angajaţilor şi contractorilor Clientului privind accesarea, actualizarea, corectarea sau ştergerea informaţiilor lor personale colectate.

## 9.3 Locaţii de Beneficiu Derivate

Când este aplicabil, taxele sunt bazate pe locaţiile pe care Clientul le identifică ca loc unde beneficiază de IBM SaaS. IBM va aplica taxele utilizând adresa de afaceri specificată ca locaţie principală de beneficiu, atunci când se comandă un IBM SaaS, cu excepţia cazului în care IBM primeşte alte informaţii de la Client. Clientul este responsabil pentru păstrarea acestor informaţii şi trimiterea oricărei modificări la IBM.

## 9.4 Livrare Continuă

Clientul are dreptul la capabilităţi şi îmbunătăţiri realizate pentru soluţie şi implementate de IBM într-un model de livrare continuă, în cloud.

## 9.5 Backup şi Restaurare

IBM Watson Health Core asigură backup-ul Datelor Clientului din mediul de producţie (inclusiv depozitele Data Lake şi Data Reservoir), aflate la ultima stare corespunzătoare cunoscută, pentru scopul serviciului de recuperare în eventualitatea defectării sistemului.

## 9.6 Disponibilitate Înaltă

Componentele IBM Watson Health Core din mediul de producţie sunt implementate în configuraţii de înaltă disponibilitate, cu servere de bază de date în cluster, pentru asigurarea redundanţei, distribuirea încărcărilor de lucru şi eliminarea punctelor unice de defecţiune.

## 9.7 Recuperarea după Dezastru

Abordarea IBM privind recuperarea după dezastru constă în mai multe centre de date, dispersate în mai multe zone geografice, pentru asigurarea obiectivelor continuităţii activităţii în mediul de producţie, după cum urmează:

- RTO – în 36 de ore de la declararea dezastrului
- RPO – nu mai mult de 24 de ore de pierdere a conţinutului Clientului

## 9.8 Instrumente de Măsură

IBM SaaS utilizează o soluţie de monitorizare sintetică, pentru urmărirea, măsurarea şi raportarea disponibilităţii şi întreruperilor, conform nivelurilor de serviciu angajate. Această soluţie simulează şi urmăreşte răspunsurile şi experienţa utilizatorilor la nivel global – atât pentru disponibilitatea statică, cât şi pentru tranzacţii.

De asemenea, IBM SaaS utilizează un sistem de monitorizare internă pentru indicii de măsurare, evenimentele şi alertele întregii soluţii.

## 9.9 Publicitate

Clientul este de acord ca IBM să poată face referire în mod public la Client, ca abonat al IBM SaaS, într-o comunicare publicitară sau de marketing.

# Anexa A

## 1. IBM Watson Health Core

IBM Watson Health Core este o platformă ca serviciu (PaaS) Activată pentru Date de Sănătate, platformă de dezvoltare şi subsistem operaţional pentru stocarea, întreţinerea şi procesarea Informaţiile Protejate privind Sănătatea (Protected Health Information - PHI), după cum sunt definite de HIPAA, şi a altor Date de Sănătate, în conformitate cu Legile Aplicabile pentru IBM privind Datele, într-un centru de date deţinut sau controlat de IBM. Clientul trebuie să achiziţioneze drepturile corespunzătoare pentru IBM Watson Health Core şi IBM Watson Health Core Access, pentru activarea caracteristicilor şi capabilităţilor descrise mai jos.

### 1.1 Mediile de Operare Watson Health Core

Dreptul Watson Health Core cuprinde trei medii de operare cloud Activate pentru Date de Sănătate, concepute pentru a-i permite Clientului să proceseze Datele de Sănătate:

- Pilot

  Furnizează un mediu sandbox în care Clienţii pot dezvolta şi testa aplicaţiile construite cu IBM SaaS. Mediul pilot implementează toate controalele de securitate HIPAA, exceptând Recuperarea după Dezastru, disponibilitatea înaltă şi backup-ul sistemelor de înregistrări.

- Mediu de Producţie

  Furnizează un mediu la scară completă, în care Clienţii pot implementa încărcările de lucru pentru Date de Sănătate. Mediul de producţie este un mediu cu înaltă disponibilitate şi încărcare echilibrată, capabil de preluare în caz de defect, într-o locaţie de Recuperare după Dezastru.

- Recuperarea după Dezastru

  Asigură o replică în oglindă a mediului Producţie şi se află într-o locaţie de centru de date separată.

### 1.2 Dezvoltarea Aplicaţiilor

IBM Watson Health Core permite dezvoltarea aplicaţiilor şi colectarea sigură a datelor de la dispozitivele Clientului sau de la dispozitivele utilizatorilor autorizaţi ai Clientului. API-urile furnizează interfeţe de program şi documentaţie pe care utilizatorii autorizaţi ai Clientului, inclusiv furnizorii de servicii terţă parte ai Clientului, le pot utiliza pentru a dezvolta aplicaţii şi a face schimb de date cu IBM SaaS. Utilizarea API-urilor de către Client sau dezvoltatorii săi este subiect al conformităţii cu Cerinţele Dezvoltatorilor privind API-urile.

- API-uri REST

  Watson Health Core furnizează o gamă de API-uri şi servicii REST pentru platforma Watson Health Core. Capabilităţile API-urilor includ, dar fără a se limita la, mecanisme pentru accesarea depozitelor de date, serviciul de îngrijire a datelor, gestionarea utilizatorilor şi istorice de auditare.

- Apple HealthKit şi Apple ResearchKit

  Watson Health Core permite integrarea cu cadrul de lucru al API-ului Apple ResearchKit, pentru studiile de cercetare bazate pe iOS, şi cu Apple HealthKit, pentru captarea datelor de sănătate.

### 1.3 Administrarea Datelor

- Gestionarea Consimţămintelor

  Watson Health Core furnizează cadrul de lucru pentru captarea consimţămintelor furnizate de pacienţi sau participanţii la studiu şi permite stocarea sigură a înregistrării consimţămintelor, separat de datele utile, atunci când o persoană se înscrie printr-o aplicaţie a Clientului activată pentru consimţăminte.

- Mascarea Datelor

  Watson Health Core furnizează abilitatea de a separa identificatorii de nume faţă de datele utile structurate. Watson Health Core primeşte datele în cloud, prin API-uri de program. API-urile permit separarea identificatorilor de nume de pacient sau de persoană faţă de restul datelor utile, pentru a fi stocate într-un depozit de date separat, criptat. Datelor utile le este alocat un jeton anonimizat, ce poate fi utilizat în viitor pentru urmărirea provenienţei.

### 1.4 Serviciile pentru Date de Sănătate

Watson Health Core asigură colectarea, stocarea şi sincronizarea datelor, inclusiv a Datelor de Sănătate exogene şi a altor Informaţii Personale, atât structurate, cât şi nestructurate.

- Preluarea Datelor

  Watson Health Core furnizează abilitatea de a prelua date de la aplicaţiile sau dispozitivele pacienţilor, prin API-uri de program. Watson Health Core permite fiecăruia dintre Indivizii Autorizaţi ai Clientului să încarce până la 25 MB de data în Health Core, în fiecare an al termenului contractual. Serviciul acceptă până la 10 încărcări per Individ per zi.

- Data Lake Operaţional

  Datele brute ale Clientului sau pacientului sunt stocate în Watson Health Core în forma lor nativă, până când sunt necesare pentru analiză şi modelare.

- Extragere, Transformare, Încărcare

  Datele sunt transformate într-un format normalizat, în cadrul sub-sistemului operaţional. O magistrală Enterprise Service Bus, bazată pe standarde specifice industriei, facilitează integrarea între diferitele aplicaţii şi protocoale ale Clientului.

- Data Reservoir

  După ce au fost pregătite, datele sunt mutate în Data Reservoir. Watson Health Core utilizează aspecte ale IBM Unified Data Model for Healthcare pentru a normaliza datele de sănătate operaţionale şi tehnice, pentru utilizarea în analize.

- Index de Persoane Master

  Watson Health furnizează instrumente de Gestionare Date Master, pentru consolidarea datelor din mai multe surse, pentru a crea o înregistrare LPR (Longitudinal Person Record).

## 2. Caracteristici Opţionale

### 2.1 IBM Watson Health Core Terminology Service

Acest serviciu add-on facilitează integrarea şi interoperabilitatea datelor, între sisteme de sănătate disparate, asigurând utilizarea unei terminologii unitare în toate aplicaţiile Watson Health Cloud. Acest serviciu furnizează platforma funcţională pentru toate task-urile ce implică terminologii, sisteme de coduri şi conţinut structurat, cum ar fi:

- crearea noilor sisteme de coduri;
- traducerea sistemelor de coduri internaţionale; şi
- asocierea listelor de coduri locale cu standardele internaţionale.

# Anexa B

IBM furnizează următorul acord privind nivelul serviciilor ("SLA") pentru IBM SaaS, după cum este specificat în PoE. SLA-ul nu este o garanţie. SLA-ul este disponibil numai pentru Client şi se aplică numai utilizării în mediile de producţie.

## 1. Credite de Disponibilitate

Rabaturile pentru disponibilitate sunt aplicabile numai pentru tarifele de abonament pentru drepturile Individ.

Clientul trebuie să înregistreze un tichet de suport Severitate 1, la help desk-ul IBM pentru suport tehnic, într-un interval de 24 de ore de la momentul în care a sesizat prima dată un eveniment care afectează disponibilitatea IBM SaaS. Clientul trebuie să asigure pentru IBM o asistenţă rezonabilă, în vederea diagnosticării şi rezolvării problemei.

Reclamaţia aferentă tichetului de suport privind neîndeplinirea SLA trebuie să fie trimisă într-un interval de trei zile lucrătoare după terminarea lunii contractate. Compensaţia pentru o reclamaţie validă privind SLA-ul va fi un credit pentru o factură viitoare pentru IBM SaaS, în funcţie de durata intervalului de timp în care nu este disponibilă procesarea sistemului de producţie pentru IBM SaaS ("Timpul de Nefuncţionare"). Timpul de Nefuncţionare este măsurat din momentul în care Clientul raportează evenimentul, până în momentul în care IBM SaaS este restaurat, fără a fi inclus timpul aferent unei întreruperi produse de mentenanţa planificată sau anunţată, de cauze care nu sunt controlate de IBM, de probleme generate de conţinutul, tehnologia, design-ul sau instrucţiunile Clientului sau ale unei terţe părţi, de platforme şi configuraţii de sistem nesuportate sau alte erori ale Clientului, de incidente de securitate cauzate de Client sau de testarea securităţii de către Client. IBM va furniza cea mai mare compensaţie aplicabilă, în funcţie de disponibilitatea cumulativă a IBM SaaS pe durata fiecărei luni contractate, aşa cum se arată în tabelul de mai jos. Compensaţia totală privind orice lună contractată nu poate depăşi 20% din a douăsprezecea parte (1/12) a tarifului anual pentru IBM SaaS.

## 2. Nivelurile de Serviciu

Disponibilitatea IBM SaaS într-o lună contractată

| **Disponibilitatea într-o lună contractată** | **Compensaţie (% din tariful de abonare lunar Individ* pentru luna contractată care face obiectul reclamaţiei)** |
|---|---|
| < 99,95% | 10% |
| < 99,0% | 20% |

* Dacă oferta IBM SaaS a fost achiziţionată de la un Partener de Afaceri IBM, tariful de abonare lunar va fi calculat în funcţie de preţul de listă din acel moment pentru oferta IBM SaaS efectivă pentru luna contractată care face obiectul reclamaţiei, cu o reducere de 50%. IBM va face un rabat disponibil în mod direct pentru Client.

Disponibilitatea, exprimată ca procentaj, este calculată astfel: numărul total de minute dintr-o lună contractată minus numărul total de minute de Timp de Nefuncţionare într-o lună contractată, împărţit la numărul total de minute din luna contractată.

Exemplu: Un total de 108 minute Timp de Nefuncţionare în luna contractată

| | |
|---|---|
| 43.200 minute într-o lună contractată de 30 de zile<br>- 108 minute Timp de Nefuncţionare<br>= 43.092 minute<br>_____<br>43.200 de minute în total | = 10% credit de Disponibilitate pentru disponibilitate de 99,75% în luna contractată |

## 3. Excluderi

Acest SLA nu se aplică pentru următoarele:

- În afară de monitorizarea serverului, SLA-ul nu se aplică pentru maşini virtuale găzduite pentru suportul aplicaţiilor personalizate şi ale Clientului.
- Cazurile în care Clientul nu şi-a îndeplinit o obligaţie importantă în baza obligaţiilor contractuale curente.

# Anexa C

Această Anexă pentru Securitate şi Continuitatea Activităţii stabileşte anumite cerinţe şi obligaţii ale privind furnizarea IBM SaaS către Client. Cerinţele şi obligaţiile specificate aici vin în completarea celor specificate în descrierea principiilor privind securitatea datelor pentru IBM SaaS, care sunt disponibile la http://www.ibm.com/cloud/data-security. Termenii scrişi cu majuscule care nu sunt definiţi aici au semnificaţiile stabilite în Contract sau Termenii de Utilizare.

## 1. Programul pentru Securitatea Informaţiilor

IBM are politici, standarde şi procese de securitate interne, bazate pe cadrul de lucru şi zonele de control ISO 27001. În plus faţă de administrarea IBM Corporate Security Organization, aceste politici, standarde şi procese sunt supuse unor auditări interne regulate.

IBM menţine un program pentru securitatea informaţiilor pentru măsurile de protecţie, la nivel organizaţional, operaţional, administrativ, fizic şi tehnic, ale procesării, stocării şi transmiterii conţinutului Clientului, care sunt cel puţin la nivelul cerinţelor din această Anexă pentru Securitate şi Continuitatea Activităţii.

IBM îi va distribui Clientului, la cererea Clientului, informaţii privind programul pentru securitatea informaţiilor IBM Watson Health, astfel încât Clientul să poată determina, în mod rezonabil, gradul de adecvare şi eficienţă al acestuia. Programul pentru securitatea informaţiilor IBM Watson Health va fi actualizat periodic, pentru a fi aliniat la practicile general acceptate în industrie şi Legile Aplicabile pentru IBM.

## 2. Controalele Accesului

IBM va dezvălui conţinutul Clientului numai către angajaţii săi, subcontractorii şi terţele părţi pentru care accesarea respectivului conţinut al Clientului este o necesitate profesională legitimă, pentru a asista IBM la îndeplinirea obligaţiilor sale faţă de Client, sau către ale persoane, după cum este necesar pentru furnizarea IBM SaaS în conformitate cu Legile Aplicabile, Contractul sau un Document Asociat, după caz. În cazul în care IBM este un Asociat de Afaceri al Clientului, IBM şi Clientul vor dezvălui Informaţii de Sănătate Personale numai în conformitate cu termenii unui Contract cu Asociatul de Afaceri aplicabil, încheiat între Părţi.

IBM are un proces formal, intern, de gestionare a accesului utilizatorilor, prin care accesul utilizatorului este solicitat formal, este aprobat în urma verificării identităţii şi este aprobat în funcţie de necesitatea informării, fiind utilizat principiul privilegiului minim. Accesul la conţinutul Clientului va fi restricţionat numai la utilizatorii activi şi conturile de utilizator active. IBM are un proces formal pentru revalidarea internă, periodică, a accesului conturilor de utilizator active.

IBM utilizează protocoale sigure de autentificare a utilizatorilor, cum ar fi alocarea identificărilor unice şi parole puternice pentru conturile de utilizator active, pe sistemele utilizate pentru a furniza servicii Clientului, în conformitate cu standardele şi politicile de securitate corporativă IBM:

a. Parolele nu vor fi cele implicite ale furnizorului şi vor fi păstrate într-o locaţie şi/sau un format care nu compromite securitatea datelor pe care le protejează.

b. Afişarea şi tipărirea parolelor se face într-un mod mascat, suprimat sau alt mod de ascundere, astfel încât părţile neautorizate să nu le poată observa şi apoi să le recompună. Nu este permisă jurnalizarea sau captarea parolelor atunci când sunt introduse. Este obligatoriu ca parolele utilizatorilor să nu fie păstrate în text clar.

c. Parolele pentru fiecare tehnologie care este inclusă în IBM SaaS sunt alese astfel încât să fie reduse riscurile asociate cu vulnerabilităţile cunoscute privind lungimea parolei şi trebuie să fie documentate.

d. Când, din motive operaţionale, este necesară utilizarea ID-urilor funcţionale partajate, interne, privilegiate, IBM gestionează ID-urile partajate, funcţionale şi/sau de sistem cu cerinţa de înregistrare la ieşire, pentru a menţine responsabilitatea individuală.

Sunt stabilite timeout-uri de inactivitate pentru toate sistemele şi aplicaţiile care stochează conţinut al Clientului.

Dacă este necesar, va fi stabilit acces de la distanţă la reţeaua, sistemele şi aplicaţiile IBM utilizate pentru stocarea conţinutului Clientului, la cererea Clientului şi în urma aprobării formale de către IBM, şi toate aceste conexiuni de la distanţă vor fi securizate utilizând protocoale puternice de autentificare şi criptare. Activitatea legată de accesul de la distanţă va fi jurnalizată şi monitorizată.

În cazul în care pentru furnizarea IBM SaaS este necesar accesul IBM de la distanţă la orice sistem din reţelele interne ale Clientului, întregul acces va fi realizat exclusiv prin utilizarea sistemelor şi protocoalelor Clientului pentru acces securizat de la distanţă şi folosind acreditările de acces primite de IBM de la Client. Accesul de la distanţă la reţeaua Clientului va fi stabilit numai la cererea IBM şi în urma aprobării de către Client, în conformitate cu politicile aplicate de Client în acel moment, care vor fi comunicate către IBM în prealabil. Utilizarea de către IBM a reţelelor interne ale Clientului va fi subiect al politicilor Clientului privind utilizarea şi securitatea IT, care vor fi furnizate către IBM în prealabil.

IBM implementează separarea sarcinilor privind administrarea securităţii, examinarea accesului şi investigările încălcărilor normelor de securitate.

Stocarea, găzduirea şi procesarea conţinutului Clientului sunt separate logic de cele ale altor clienţi cărora IBM le furnizează servicii. În cazurile în care Clientul a autorizat o zonă de lucru partajată pentru stocare, găzduire sau procesare, IBM va aplica proceduri şi măsuri de protecţie, în conformitate cu cerinţele stabilite în această Anexă pentru Securitate şi Continuitatea Activităţii, concepute pentru a împiedica dezvăluirea neautorizată a conţinutului Clientului.

IBM implementează măsuri "clean desk" sau "clear screen", pentru a nu fi lăsat conţinutul Clientului nesupravegheat, în niciun loc public şi în niciun moment.

## 3. Transferul şi Criptarea

IBM va lua măsuri de precauţie corespunzătoare la transmiterea conţinutului Clientului (prin fax, e-mail, curier etc.), pentru a se asigura că sunt utilizate informaţii de contact corecte pentru destinatar, aranjând în prealabil cu destinatarul respectiv primirea în siguranţă a informaţiilor.

IBM utilizează, şi va determina Personalul IBM să utilizeze, forme corespunzătoare de criptare sau alte tehnologii de securizare, în orice moment al procesării conţinutului Clientului, precum şi pentru orice transfer, comunicare, acces de la distanţă sau stocare (inclusiv stocare de backup) a conţinutului Clientului. De exemplu, IBM va cripta, utilizând o criptare bazată de un standard corespunzător din industrie, toate înregistrările şi fişierele în care este inclus conţinut al Clientului:

a. stocate pe laptop-uri, dispozitive portabile sau medii electronice portabile IBM, inclusiv benzi de backup, în tranzitul către o locaţie de stocare externă;

b. stocate sau transportate de IBM în afara birourilor şi clădirilor securizate fizic ale Clientului sau ale IBM, cu excepţia documentelor tipărite pe hârtie;

c. în timpul trimiterii prin reţele publice de către IBM;

d. în timpul transferării de pe sistemele IBM către Client;

e. în timpul transmiterii wireless de către IBM; şi

f. stocate de IBM pe servere şi în baze de date.

## 4. Securitatea Reţelei

IBM utilizează versiuni, actualizate rezonabil, de software pentru securitatea sistemelor, cum ar fi firewall-uri, proxy-uri, firewall-uri şi interfeţe de aplicaţie web. Un astfel de software trebuie să include protecţie contra malware-ului, precum şi patch-uri şi definiţii de virus actualizate rezonabil. În conformitate cu standardele corporative, trebuie să fie instalat software antivirus pe staţiile de lucru, serverele şi terminalele unde este posibil din punct de vedere tehnic, iar software-ul este gestionat conform politicii corporative, cu soluţii de gestionare internă.

IBM monitorizează IBM SaaS pentru a detecta şi identifica incidentele de securitate cât mai devreme posibil. IBM va menţine, cel puţin, măsuri de prevenire şi instrumente de detectare a intruziunilor bazate pe standarde ale industriei, monitorizarea şi procese de reacţie, într-o manieră concepută pentru a identifica vulnerabilităţile şi riscurile interne şi externe care ar putea avea ca rezultat dezvăluirea neautorizată, utilizarea necorespunzătoare, alterarea sau distrugerea conţinutului Clientului sau a sistemelor de informaţii care sunt utilizate pentru a furniza servicii Clientului.

IBM se abonează la servicii de informaţii privind vulnerabilităţile sau de consiliere privind securitatea informaţiilor şi la alte surse relevante pentru obţinerea ultimelor informaţii privind vulnerabilităţile sistemelor. IBM realizează în mod regulat evaluări ale vulnerabilităţilor şi remedierea problemelor reţelei.

IBM monitorizează IBM SaaS pentru a detecta, identifica, limita şi rezolva Incidentele de Securitate.

IBM validează disponibilitatea, integritatea şi eficienţa infrastructurii pentru securitatea reţelei utilizate pentru a face disponibil IBM SaaS, prin procesul IBM de gestionare a ediţiilor.

## 5. Gestionarea Incidentelor şi Notificările

Echipa IBM Watson Health colaborează cu IBM Cybersecurity Incident Response Team, o echipă globală care gestionează primirea, investigarea şi coordonarea internă a incidentelor de securitate legate de ofertele IBM şi care implementează măsuri preventive, pentru a reduce problemele de securitate privind software-ul. Un "Incident de Securitate" o acţiune reuşită de accesare, utilizare, dezvăluire, modificarea sau interferenţă neautorizată cu operaţiunile sau datele de sistem, într-un sistem de informaţii utilizat de IBM pentru a furniza IBM SaaS. Dacă este descoperit un Incident de Securitate (prin scanarea de rutină, alerte, evenimente de prag etc.), IBM va informa Clientul şi îi va trimite o notificare:

a. privind orice Incident de Securitate confirmat ce implică un conţinut al Clientului, imediat ce este posibil, dar nu mai târziu de 2 zile lucrătoare de la investigarea şi confirmarea unui astfel de Incident de Securitate;

b. cu promptitudine după orice cerere de acces la sau de informaţii despre orice conţinut al Clientului, de la orice oficial guvernamental (inclusiv orice agenţie de protecţie a datelor sau de aplicare a legii), exceptând cazul în care este interzis de lege sau de o hotărâre relevantă; şi

c. exceptând cele permise în secţiunea intitulată Controalele Accesului din această Anexă pentru Securitate şi Continuitatea Activităţii, înainte de orice dezvăluire, transferare sau accesare a conţinutului Clientului de către o terţă parte.

## 6. Jurnalizarea

IBM menţine, în conformitate cu politicile şi practicile IBM şi practicile general acceptate în industrie, o monitorizare rezonabilă a sistemelor, pentru utilizarea sau accesarea neautorizată a Datelor Procesate ale Clientului. Încălcările măsurilor de securitate, realizate sau încercate, privind logarea sau accesarea, vor fi jurnalizate.

IBM menţine înregistrări ale tuturor cererilor de acces şi istorice ale activităţilor la accesare, pentru toate sistemele care stochează, accesează, procesează şi transmit date ale Clientului şi Date de Sănătate, atât timp cât se specifică în HIPAA şi în alte Legi Aplicabile pentru IBM privind Datele.

Istoricele şi rapoartele includ, cel puţin: (i) toate tentativele de logare, indiferent că au reuşit sau nu, inclusiv informaţii rezonabile de identificare; (ii) toate modificările de configuraţie ale sistemului şi reţelei, inclusiv instalările de aplicaţii, modificările de gestionare a utilizatorilor şi modificările permisiunilor de acces la fişiere; (iii) tentativele de accesare a resurselor, indiferent că au reuşit sau nu, inclusiv tentativele de a accesa orice fişier, partajare de reţea, istoric sau altă resursă; şi (iv) descărcările de date, inclusiv tipul de conţinut al datelor şi protocolul de acces utilizat pentru a realiza descărcarea.

## 7. Dezvoltarea Aplicaţiilor Software şi Gestionarea Modificărilor

IBM respectă practicile sigure de dezvoltare a aplicaţiilor şi de codare, care protejează integritatea aplicaţiilor de producţie şi codului sursă asociat faţă de modificările neautorizate şi netestate.

IBM respectă procesul de gestionare a modificărilor, care include (a) înregistrarea şi aprobarea formală a modificărilor şi proceduri back-out; şi (b) testarea corespunzătoare a modificărilor, inclusiv acceptarea de către utilizator a rezultatelor testării, precum şi testarea securităţii.

IBM respectă procesul de gestionare a patch-urilor, care include testarea patch-urilor înainte de a le instala pe toate sistemele utilizate pentru stocarea, accesarea şi transmiterea conţinutului Clientului sau utilizate pentru a livra către Client servicii, inclusiv IBM SaaS.

IBM le impune administratorilor de sistem menţinerea unor informaţii complete, precise şi actualizate privind configuraţia tuturor sistemelor de informaţii utilizate pentru stocarea, accesarea şi transmiterea conţinutului Clientului.

## 8. Securitatea Fizică şi de Mediu

Platforma IBM Watson Health Core este implementată pe infrastructura de date IBM SoftLayer. IBM SoftLayer menţine securitatea fizică şi de mediu, controlul accesului, controalele şi procesele pentru protejarea datelor Clientului faţă de încălcările privind oamenii, mediul şi tehnice sau impactul acestora.

Accesul general în clădirile în care este găzduit IBM SaaS este controlat cu un sistem de acces bazat pe carduri. Peste tot în clădire sunt montate camere ale unui sistem de televiziune cu circuit închis şi

acestea sunt urmărite de personalul de securitate. Uşile de acces selectate sunt dotate cu alarme, care sunt supravegheate de personalul de securitate.

Accesul la zonele controlate este restricţionat prin utilizarea accesului pe bază de card şi/sau verificare biometrică. Persoanele care nu au acces autorizat la zonele controlate trebuie să trebuie să se autentifice şi sunt escortate de o persoană cu acces aprobat la zona controlată. Toate ieşirile de urgenţă ale zonei controlate au alarme audio, care sunt supravegheate de personalul de securitate. Periodic, se verifică funcţionarea alarmelor şi rezultatele sunt înregistrate şi păstrate. Drepturile de acces la zonele controlate sunt revalidate complet, trimestrial. La terminarea angajării, accesul la zonele controlate este revocat.

Clădirile sunt protejate faţă de factori de mediu, cum ar fi focul, apa şi căldura, cu alarme de incendiu, extinctoare, alarme de fum şi sisteme de stingere a incendiilor. Clădirile sunt protejate faţă de întreruperile sau căderile de tensiune prin sisteme UPS (Uninterruptible Power Supply) şi generatoare de rezervă, care sunt întreţinute şi testate cu regularitate.

Informaţii şi rapoarte privind conformitatea IBM SoftLayer pot fi găsite la: http://www.softlayer.com/compliance.

## 9. Continuitatea Activităţii

IBM are planuri de asigurare a continuităţii activităţii şi recuperare după dezastru, care sunt concepute pentru a menţine un nivel al serviciului conform cu obligaţiile stabilite în Contract. Astfel de planuri pentru continuitatea activităţii şi recuperarea după dezastru trebuie să fie actualizate şi testate periodic (cel puţin o dată pe an). IBM va implementa toate modificările rezonabile privind planurile pentru continuitatea activităţii şi recuperarea după dezastru, pentru a asigura conformitatea cu practicile general acceptate în industrie, în fiecare caz, fără o interferenţă nerezonabilă cu IBM SaaS sau mediul de producţie utilizat de Client.

În eventualitatea unui dezastru care face ca IBM SaaS să devină indisponibil pentru Client, IBM va notifica imediat Clientul şi va activa planul pentru continuitatea activităţii şi/sau recuperarea după dezastru. când este declarat un dezastru, obiectivul continuităţii activităţii IBM SaaS este de a restaura accesul Clientului la IBM SaaS, după cum urmează: În eventualitatea unei întreruperi a alimentării electrice, obiectivul RTO (Recovery Time Objective) pentru restaurarea mediului de producţie IBM Watson Health este un interval de 36 de ore de la declararea dezastrului. Obiectivul RPO (Recovery Point Objective) este de maximum 24 de ore de pierdere a conţinutului Clientului în mediul de producţie. Obiectivele specifice privind continuitatea pentru soluţiile Watson Health pot varia.

Abordarea IBM privind recuperarea după dezastru constă în mai multe centre de date, dispersate în mai multe zone geografice.

Toate centrele de date IBM SoftLayer menţin mai multe surse de alimentare electrică, legături prin cabluri cu fibre optice, generatoare dedicate şi baterii de rezervă. Ele sunt construite cu hardware şi echipamente de top în industrie, asigurând cel mai înalt nivel de performanţă, fiabilitate şi interoperabilitate. Toate componentele care urmează să fie incluse în centrul de date, de exemplu resurse de alimentare electrică şi răcire pentru redundanţa n+1, sunt inspectate pentru asigurarea stabilităţii în centrele de date.

## 10. Conformitatea

Practicile de securitate IBM se bazează pe ISO 27001-27002. Aceste practici asigură controlul structurilor pentru, dar fără a se limita la, Analiza Riscurilor, Securitatea Fizică, Planificarea pentru Urgenţe, Investigaţiile, Protecţia Informaţiilor, Educaţia, Protecţia Datelor şi Operaţiunile.

IBM examinează activităţile legate de securitate şi confidenţialitate, pentru verificarea conformităţii cu practicile de securitate IBM.

IBM respectă Legile Aplicabile pentru IBM privind Datele, din Jurisdicţiile Incluse în Scop.

Tratarea corespunzătoare a informaţiilor confidenţiale ale Clienţilor este stipulată în IBM Business Conduct Guidelines, un document pe care toţi angajaţii trebuie să-l revadă anual (şi apoi să se certifice) .

## 11. Diverse

IBM se va asigura că acordurile sale cu toţi subcontractorii şi/sau terţele părţi angajate în furnizarea IBM SaaS conţin termeni care, ca nivel minim, protejează conţinutul Clientului, cum sunt cei din această Anexă pentru Securitate şi Continuitatea Activităţii, şi orice Document Asociat aplicabil, în măsura în care aceşti termeni sunt aplicabili pentru servicii ce urmează să fie realizate de respectivii subcontractori şi/sau terţe părţi.